

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215279

(43)Date of publication of application : 04.08.2000

(51)Int.Cl.

G06K 17/00

G07D 9/00

G07F 7/12

G07F 7/08

(21)Application number : 11-017174

(71)Applicant : HITACHI LTD

HITACHI VIDEO & INF SYST INC

(22)Date of filing : 26.01.1999

(72)Inventor : MATSUMOTO KENJI

ITO SHIGEYUKI

TAKAMI MINORU

INOUE MASAYUKI

YONEDA KOICHI

INAMITSU TETSUJI

YAMAUCHI TSUKASA

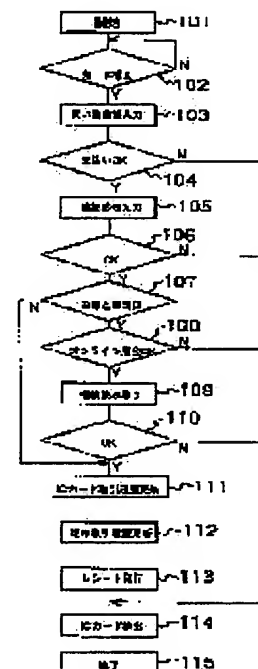
INOUE YOSHITAKE

(54) IC CARD SETTLEMENT DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To dynamically optimize the relation between the cost required for identity certification and the certainty of identity certification in accordance with a value which is to be protected by identity certification.

SOLUTION: The input of a shopping amount and a password is received (steps 103 and 105). When the shopping amount is lower than a setting value (Step 107), settlement is executed (steps 111 and 112) if the inputted password matches with a password stored in an IC card. When the shopping amount is higher than the setting value (step 107), the fingerprint of a user is read (step 109) and settlement is executed (steps 111 and 112) only when the fingerprint which is read matches with a fingerprint stored in the IC card (S110).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-215279

(P2000-215279A)

(43)公開日 平成12年8月4日(2000.8.4)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 K 17/00		G 0 6 K 17/00	L 3 E 0 4 0 S 3 E 0 4 4 V 5 B 0 5 8
G 0 7 D 9/00	4 3 6 4 6 1	G 0 7 D 9/00	4 3 6 Z 4 6 1 A
審査請求 未請求 請求項の数12 O L (全 22 頁) 最終頁に続く			

(21)出願番号 特願平11-17174

(22)出願日 平成11年1月26日(1999.1.26)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71)出願人 000233136

株式会社日立画像情報システム

神奈川県横浜市戸塚区吉田町292番地

(72)発明者 松本 健司

神奈川県横浜市戸塚区吉田町292番地 株

式会社日立製作所マルチメディアシステム

開発本部内

(74)代理人 100087170

弁理士 富田 和子

最終頁に続く

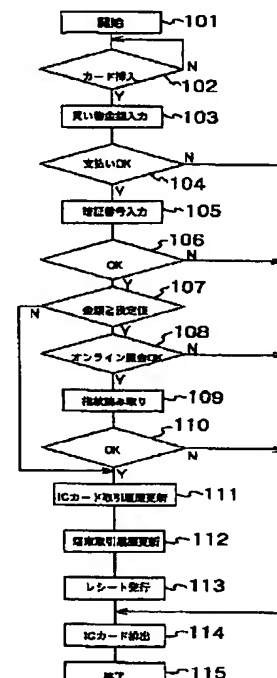
(54)【発明の名称】 ICカード決済装置

(57)【要約】

【課題】本人認証に要するコストと本人認証の確度との関係を本人認証によって守るべき価値に応じて動的に最適化する。

【解決手段】買い物金額と暗証番号の入力を受け付け(ステップ103、105)、買い物金額が設定値より低額である場合(ステップ107)は、入力された暗証番号とICカードに記憶された暗証番号が一致すれば(ステップ106)、決済を行う(ステップ111、112)。一方、買い物金額が設定値より高額である場合(ステップ107)は、利用者の指紋を読み取り(ステップ109)、読み取った指紋とICカードに記憶された指紋が一致した場合にのみ(ステップ110)、決済を行う(ステップ111、112)。

図3



【特許請求の範囲】

【請求項1】 ICカードの正当な所有者の暗証番号と生体情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置であって、

決済を行う金額の入力を受け付ける決済額受け付け手段と、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

入力された決済を行う金額が所定値より低額である場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第1決済手段と、

入力された決済を行う金額が所定値より高額である場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第2決済手段とを有することを特徴とするICカード決済装置。

【請求項2】 ICカードの正当な所有者の暗証番号と、生体情報と、ICカードを用いた決済の回数を算出可能な当該ICカードを用いた決済の履歴情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置であって、

決済を行う金額の入力を受け付ける決済額受け付け手段と、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

ICカードに記憶された履歴情報から求まる当該ICカードを用いた決済の回数が所定値を超えない場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第1決済手段と、

ICカードに記憶された履歴から求まる当該ICカードを用いた決済の回数が所定値を超える場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第2決済手段と、

決済が行われた場合に、行われた決済の内容に応じてICカードに記憶された履歴情報を更新する履歴情報更新手段とを有することを特徴とするICカード決済装置。

【請求項3】 ICカードの正当な所有者の暗証番号と、生体情報と、ICカードを用いた決済の金額の累計を算出可能な当該ICカードを用いた決済の履歴情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置であって、

決済を行う金額の入力を受け付ける決済額受け付け手段と、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

ICカードに記憶された履歴情報から求まる当該ICカードを用いた決済の金額の累計が所定値を超えない場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第1決済手段と、

10 ICカードに記憶された履歴から求まる当該ICカードを用いた決済の金額の累計が所定値を超える場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第2決済手段と、

決済が行われた場合に、行われた決済の内容に応じてICカードに記憶された履歴情報を更新する履歴情報更新手段とを有することを特徴とするICカード決済装置。

【請求項4】 請求項1、2または3記載のICカード決済装置であって、

20 前記第2決済手段は、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号とが一致し、かつ、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報とが一致した場合にのみ決済を行うことを特徴とするICカード決済装置。

【請求項5】 請求項1、2、3または4記載のICカード決済装置であって、

30 前記第1決済手段は、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号とが一致しない場合には、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行うことを特徴とするICカード決済装置。

【請求項6】 ICカードの正当な所有者の暗証番号と生体情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置であって、

ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、

40 ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、

前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、両暗証番号が一致しない場合に、さらに、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う決済手段とを有することを特徴とするICカード決済装置。

【請求項7】 請求項1、2、3、4、5または6記載のICカード決済装置であって、

50 ICカード使用者から、今後使用を希望する新しい暗証番

号の入力を受け付ける新暗証番号受け付け手段と前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合にICカードに記憶された暗証番号を、新暗証番号受け付け手段が受け付けた新しい暗証番号に更新する暗証番号更新手段とを有することを特徴とするICカード決済装置。

【請求項8】請求項1、2、3、4、5、6または7記載のICカード決済装置であって、前記生体情報は、指紋の情報であることを特徴とするIC

カード決済装置。
【請求項9】ICカードに記憶された当該ICカードの正当な所有者の暗証番号と指紋情報とを用いて、ICカード使用者の認証を行なうICカード処理装置であって、ICカード使用者より、指先による暗証番号の入力を受け付ける入力部と、当該入力部に暗証番号入力のために置かれた指先から指紋情報を読み取る読み取り部とを有することを特徴とするICカード処理装置。

【請求項10】ICカードの所有者の個人情報記憶されたICカードを処理するICカード処理装置であって、ICカード使用者に、サービスを提供するためのユーザインタフェースを供する手段と、ICカードに記憶された個人情報に応じて、ICカード使用者に供するユーザインタフェースをカスタマイズする手段とを有することを特徴とするICカード処理装置。

【請求項11】ICカードの正当な所有者の暗証番号と生体情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置において、ICカード使用者を認証する方法であって、ICカードの不正使用による損害の可能額が低額である場合に、ICカード使用者より受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、ICカードの不正使用による損害の可能額が高額である場合に、ICカード使用者より読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第2決済手段とを有することを特徴とするICカード使用者を認証する方法。

【請求項12】ICカードの正当な所有者の暗証番号と個人情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置において、ICカード使用者を認証する方法であって、ICカードの不正使用による損害の可能額が低額である場合に、ICカード使用者より受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、ICカードの不正使用による損害の可能額が高額である場合に、ICカード使用者より受け付けた個人情報とICカードに記憶された個人情報との一致を調べ、両個人情報一致した場合に決済を行う第2決済手段とを有することを特徴とするICカード使用

者を認証する方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クレジット情報や電子マネー情報などを格納したICカードを用いた決済を行うICカード決済装置に関するものである。

【0002】

【従来の技術】現在、取引者間の現金以外の取引の決済の方法としては、クレジットカードによる決済が一般的である。また、クレジットカードとしては、磁気ストライプカードを使用した物が主流であり、その決済の手順は一般的には次のようなものである。

【0003】すなわち、まず、買い物時に購入者が販売者にクレジットカードを渡す。販売者は、磁気ストライプリーダーを用いて磁気ストライプに格納されているカードのクレジット番号を読み出す。その後、電話回線を使用してクレジットカードの照会センタに接続し、読み取ったクレジット番号をオンラインで照会する。そして、照会の結果、過去に、このクレジットカードによるに不正な買い物が無いことが確認されると、購入者のサインによりカード所有者本人であることを確認し、クレジットによる販売を行い、販売の内容をクレジット会社に通知する。この場合、後日、販売者への支払いはクレジット会社より、購入者の支払いはクレジット会社に対して行われる。

【0004】このような従来のクレジットカードを利用した決済の方法は、クレジットカードの偽造、盗難、サインの模倣などによるクレジットカードの不正使用が行われることを十分に防止することができなかった。また、前述したオンライン照会によって、クレジットカードの不正使用が繰り返されることを防止する技術も、実際には、少額取引の場合には販売者がオンライン照会を省略してしまうことがあるため、必ずしも常に有効に機能しているとは言えなかった。

【0005】さて、最近ではICカードを使用した新しい決済方法が、さかんに提案、実験されている。

【0006】その一つが、クレジットカードを、ICカード化したものであり、他の一つが、ICカードを使用した電子マネーである。ICカード内のメモリに電子マネーを格納し、取引時には、現金の代わりに、ICカード間で電子マネーをやりとりしようとするものである。

【0007】そして、いずれの場合も、ICカードの不正使用を防ぐためには、ICカード使用者がICカードの正当な所有者であることを確認する本人認証が重要となる。

【0008】このようなICカード所有者の本人認証を行う技術としては、ICカード内にICカード所有者の暗証番号をICカード外から知ることができないように記録しておき、決済時には、ICカード決済装置にICカードを装着し、ICカードにおいて、ICカード使用者がICカード決済装置に入力した暗証番号と、装着されたICカードに記録

された暗証番号とを照合し、一致した場合に、本人と認証しようとするものがある。これは、従来のクレジットカードのサインの代わりに暗証番号を使用しようとするものであり、この技術は、利用者が、取引のたびに、いちいちサインする手間を不要とすることができると共に、暗証番号をICカード外から知ることができないようにICカードに記憶するため、この暗証番号をサインのように、簡単に第三者が知ることができないという点で、従来のクレジットカードより優れている。

【0009】また、ICカード所有者の本人認証を行う技術としては、ICカード内にICカード所有者の生体情報を記録しておき、決済時には、ICカード決済装置にICカードを装着し、ICカード決済装置において、ICカード使用者からICカード決済装置に生体情報を取り込み、装着されたICカードに記録された生体情報と照合し、一致した場合に、本人と認証しようとするものがある。これは、従来のクレジットカードのサインの代わりに生体情報を使用しようとするものであり、この技術は、利用者が暗証番号を覚える必要がなく、生体情報が、正当なICカード所有者独自かつ不可分のものであることより、より高い精度で本人認証を行えることが期待できる点で、暗証番号を用いる技術より優れている。なお、生体情報の代表的なものとしては、指紋、掌紋、虹彩、網膜などの形状がある。

【0010】

【発明が解決しようとする課題】前記ICカードの本人認証に暗証番号を用いる技術によれば、もし暗証番号が盗まれた場合に、ICカードの不正使用を防ぐことができなくなるという問題がある。一方、前記ICカードの本人認証に生体情報を用いる技術によれば、生体情報の照合に必要な処理の処理量が多いこと、決済時毎に生体情報の取得を行わなければならないことなどより、本人認証に必要となる処理時間、利用のコストが大きくなってしまいうという問題がある。

【0011】すなわち、ICカードの本人認証を高い確度で行おうとすると高コストとなり、低コストでICカードの本人認証を行おうとすると本人認証の確度は低くなるという関係が生じる。そして、このようにコストと確度はトレードオフの関係にあるため、どのようなコストをかけてどのような確度で本人認証を行うかは、本人認証によって守るべき価値に応じて最適化するのが合理的であるが、電子マネーやクレジットカードの場合、本人認証によって守られる価値は、個々のICカードの利用状況によって刻々変化するため、前述した暗証番号と生体情報の一方、もしくは、両方を用いることによって、このような最適化を行うことができない。

【0012】そこで、本発明は、本人認証に要するコストと本人認証の確度との関係を本人認証によって守るべき価値に応じて動的に最適化することができるICカード決済装置を提供することを課題とする。

【0013】また、前記ICカードの本人認証に暗証番号を用いる技術によれば、ICカードの正当な所有者が暗証番号を忘れてしまった場合には、正当な所有者であっても、ICカードを使用できなくなってしまうという問題がある。そこで、本発明は、正当な所有者であれば、暗証番号を忘れてしまった場合でも、ICカードを利用可能とすることのできるICカード決済装置を提供することを課題とする。

【0014】また、前記ICカードの本人認証に生体情報を用いる技術によれば、決済時の生体情報の取得、たとえば、指紋の取得に際し、ICカードの所有者に不快感を与えてしまうという問題がある。

【0015】そこで、本発明は、生体情報の取得に際して、ICカードの所有者に与える不快感を軽減することも課題とする。

【0016】

【課題を解決するための手段】前記課題達成のために本発明は、たとえば、ICカードの正当な所有者の暗証番号と生体情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置であって、決済を行う金額の入力を受け付ける決済額受け付け手段と、ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、入力された決済を行う金額が所定値より低額である場合に、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行う第1決済手段と、入力された決済を行う金額が所定値より高額である場合に、前記生体情報読み取り手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う第2決済手段とを有することを特徴とするICカード決済装置を提供する。

【0017】このようなICカード決済装置によれば、低額の決済時には、暗証番号のみの迅速な本人認証を、高額の決済時には、生体情報を用いた確度の高い本人認証を行うので、本人認証によって守るべき価値の一つ、すなわち、決済がICカードの不正使用である場合の損害額となる決済金額に応じて、動的に本人認証の確度とコストを最適化することができる。

【0018】また、本発明は、前記課題達成のために、たとえば、ICカードの正当な所有者の暗証番号と生体情報とが記憶されたICカードを用いて、商取引の決済を行うICカード決済装置であって、ICカード使用者から、暗証番号の入力を受け付ける暗証番号受け付け手段と、ICカード使用者から、生体情報を読み取る生体情報読み取り手段と、前記暗証番号受け付け手段が受け付けた暗証番号とICカードに記憶された暗証番号との一致を調べ、両暗証番号が一致した場合に決済を行い、両暗証番号が一致しない場合に、さらに、前記生体情報読み取り

手段が読み取った生体情報とICカードに記憶された生体情報との一致を調べ、両生体情報が一致した場合に決済を行う決済手段とを有することを特徴とするICカード決済装置を提供する。

【0019】このようなICカード決済装置によれば、通常の決済時は暗証番号を用いた本人認証により迅速に決済を行うことができると共に、暗証番号を知らない、すなわち、疑義あるユーザに対しては、本人認証を生体情報を用いた本人認証により高い確度で行って、決済処理を行うことができるようになる。逆の見方をすれば、正

当なユーザは暗証番号をもし忘れても、ICカードによる買い物をすることができるようになる。

【0020】また、本発明は、前記課題達成のために、ICカードに記憶された当該ICカードの正当な所有者の暗証番号と指紋情報とを用いて、ICカード使用者の認証をおこなうICカード処理装置であって、ICカード使用者より、指先による暗証番号の入力を受け付ける入力部と、当該入力部に暗証番号入力のために置かれた指先から指紋情報を読み取る読み取り部とを有することを特徴とするICカード処理装置を提供する。

【0021】このようなICカード処理装置によれば、ICカード使用者に指紋情報の読み取りを意識させることなく、ICカード使用者が暗証番号を入力時に指紋情報を読み取ることができる。したがって、指紋読み取り時のICカード使用者の不快感を軽減することができる。

【0022】

【発明の実施の形態】以下、本発明の一実施形態について説明する。

【0023】まず、第1の実施形態について説明する。

【0024】図1に、本実施形態に係るICカード決済端末の構成を示す。

【0025】本ICカード決済端末は、クレジット決済処理を行うクレジット端末であり、図中、1はクレジット端末、10はクレジット端末1にリムーバブルに装着されるICカードである。また、クレジット端末1中、2はキー入力部、3は表示部、4はレシート印刷部、5は演算処理部、6はクレジットセンタと接続するためのモデム部、7は取引履歴情報記憶部、8はICカード読み書き部、9は指紋読み取り部である。また、ICカード10中、11は接続部、12は演算処理部、13は取引履歴情報記憶部、14はID情報記憶部、15は暗証番号記憶部、16は指紋情報記憶部である。

【0026】ここで、ID情報記憶部14には各ICカード毎に固有のクレジット番号が格納されており、暗証番号記憶部15にはユーザーが登録した暗証番号が格納されており、指紋情報記憶部16にはユーザーが登録した指紋の情報が格納されている。

【0027】次に、ICカード10の取引履歴情報記憶部13には図2に示す取引履歴情報が蓄積される。

【0028】図示するように取引履歴情報は、買い物し

た取引日、買い物金額、累積金額、累積回数よりなる。これらは、このICカードによるクレジットによって買い物をすると、その決済を行ったクレジット端末1により格納される。ここで、累積金額は、このICカードによるクレジットによって行った買い物の買い物金額の累積であり、累積の購入回数はこのICカードによるクレジットによって行った買い物の回数である、ただし、後述するように、累積金額と累積回数は、このICカードによるクレジットによって買い物の決済を行うクレジット端末1が、このICカードのクレジット番号をクレジットセンタに照会して、過去の不正使用がないことを確認できた場合に初期化され、次の買い物では累積回数は1、累積金額は当該次の買い物金額となる。図の例は、No. 7、4の買い物のときに、その決済を行ったクレジット端末1が、このICカードのクレジット番号をクレジットセンタに照会して、過去の不正使用がないことを確認した場合を示している。

【0029】以下、本実施形態に係るクレジット端末1の動作について説明する。

20 【0030】図3に、クレジット端末1の演算処理部5が行う決済時の動作の手順を示す。

【0031】図示するように、クレジット端末1の演算処理部5は、ユーザーがICカード10をクレジット端末1に挿入することにより装着すると（ステップ102）、ICカード読み書き部8にICカード10に電源、クロック、リセット信号を供給させ、ICカードを活性化させる。この結果、クレジット端末10の演算処理部5は、接続部11、ICカード読み書き部8を介してICカード内の情報を読み出すことが可能となる。

30 【0032】次に、店員が買い物金額を入力部2よりクレジット端末に入力すると（ステップ103）、演算処理部5は、まず始めに支払いを行うかどうかの確認画面を表示部3に表示させる（ステップ104）。そして、ユーザーが支払いを行うことを入力部2より選択した場合は、さらに、入力部2よりユーザからの暗証番号の入力を受け付ける（ステップ105）。一方、ユーザーが支払いを行わないことを入力部2より選択した場合には、ICカード読み書き部8にICカード10を排出させ（ステップ114）、処理を終了する（ステップ115）。

40 【0033】ステップ105で暗証番号が入力されると、演算処理部5は、ICカード10の演算処理部12に暗証番号を渡し、入力された暗証番号と、ICカード10の暗証番号記憶部15に格納された番号とを比較させ、その結果より両者が一致したかを確認する（ステップ106）。そして、一致を確認できなかった場合には、ICカード読み書き部8にICカード10を排出させ（ステップ114）、処理を終了する（ステップ115）。

50 【0034】一方、ステップ106で、暗証番号の一致を確認できた場合には、その後、買い物金額があらか

め設定した金額値を超えるかどうかの判定を行う（ステップ107）。そして、買い物金額があらかじめ設定した金額値を超えていない場合には、本人認証が成立したものとステップ111に進む。

【0035】一方、ステップ107で買い物金額が設定値を超えていると判定された場合には、ここでクレジットセンタにオンライン照会を行い、ユーザーの使用するICカードで過去に不正な使用がないかを確認する（ステップ108）。この場合、モデム6を介して電話回線によりクレジットセンタとデータのやり取りを行う。そして、過去に不正な使用がないことを確認できなかった場合には、ICカード10を排出し（ステップ114）、処理を終了する（ステップ115）。

【0036】一方、ステップ108で、過去に不正な使用がないことを確認できた場合には、指紋読み取り部9によりユーザーの指紋を読み取る（ステップ109）。そして、演算処理部5は、ICカード10の演算処理部12に読み取った指紋の情報を渡し、これと、ICカード10の指紋情報記憶部16に格納された指紋情報とを比較させ、その結果より両者が一致したかを確認する（ステップ110）。そして、一致を確認できなかった場合には、ICカード読み書き部8にICカード10を排出させ（ステップ114）、処理を終了する（ステップ115）。

【0037】一方、ステップ110で指紋の一致を確認できた場合には、本人認証が成立したものとステップ111に進む。

【0038】本人認証が成立した場合に実行されるステップ111では、買い物金額、今日の日付に応じて、ICカードの取引履歴情報記憶部13の取引履歴情報を更新する。

【0039】また、クレジット端末側1の取引履歴情報記憶部7も更新する（ステップ112）。なお、クレジット端末側1の取引履歴情報記憶部7には、買い物の日付、買い物金額、買い物に使われたICカード10のクレジット番号などを記憶する。

【0040】そして、印刷部4によりレシートを発行する（ステップ113）と共に、ICカード10を排出して（ステップ114）、処理を終了する（ステップ115）。

【0041】なお、ステップ111でのICカードの取引履歴情報記憶部13の取引履歴情報の更新では、前述したように、累積金額、累積回数も更新する。また、前述したように、累積金額、累積回数はステップ108で過去に不正な使用がないことを確認できた場合には、次の買い物の際に初期化するが、これは、たとえば、ステップ108で過去に不正な使用がないことを確認できた場合に、その旨を、取引履歴情報記憶部13の取引履歴情報の過去に不正な使用がないことを確認した買い物に対応づけて記憶し、ステップ111において前回の買い

物に対応づけて過去に不正な使用がないことを確認できたことが記憶されている場合には、ステップ111のICカードの取引履歴情報記憶部13の取引履歴情報の更新において、累積金額、累積回数を初期化するようにすればよい。または、ステップ108で過去に不正な使用がないことを確認できた場合に、その時の取り引き終了時に、取引履歴情報記憶部13の取引履歴情報を消去するようにしてもよい。

【0042】以上、本発明の第1の実施形態について説明した。

【0043】以上のように、本第1実施形態では、買い物金額が設定値以下の場合には暗証番号により本人認証が行われるが、この場合はオンライン照会が行われないため、短時間で処理を終わらせることができる。一方、買い物金額が設定値を超える場合は、オンライン照会が行われると共にユーザーの指紋により再度本人認証が行われるため、カードと暗証番号を盗まれて悪用された場合にも不正使用を防ぐことができる。すなわち、本第1実施形態によれば、低額な買い物時には、暗証番号のみの迅速な本人認証を、高額な買い物時には、指紋を用いた確度の高い本人認証を行うので、本人認証によって守るべき価値の一つ、すなわち、買い物がICカードの不正使用である場合の損害額となる買い物金額に応じて、動的に本人認証の確度とコストを最適化することができる。

【0044】なお、指紋情報の確認に関しては、セキュリティの面では安全であるため、以上の説明では、ICカード内の演算処理部12で比較を行うものとした。しかしながら、処理時間などで問題がある場合は、クレジット端末内の演算処理部5で処理を行うようにすることもできる。

【0045】以下、本発明の第2の実施形態について説明する。本第2実施形態は、前記第1実施形態における図3の処理を、図4に示すように、買い物金額が設定値を超えた場合のみならず、累積金額が設定値を超えた場合（ステップ201）と、累積回数が設定値を超えた場合（ステップ202）にも、オンライン照会（ステップ108）と、指紋の比較（ステップ109、110）を行い、その結果、過去の不正無しと指紋の一致が確認できたならば本人認証が成立したとするようにしたものである。

【0046】本第2実施形態によれば、前記第1実施形態の効果に加え、累積金額が設定値を超えた場合と、累積回数が設定値を超えた場合にも指紋を用いた確度の高い本人認証を行う。ここで、累積金額や累積回数は、そのICカードが不正使用され続けた場合の損害額の大きさに比例するものと推定できるので、本第2実施形態によれば、前記第1実施形態に対し、さらに、本人認証によって守るべき価値の一つである、連続不正使用による損害額の大きさに応じて、動的に本人認証の確度とコストを最適化することができる。

【0047】なお、以上の第1、第2本実施形態では、買い物金額、累積金額、累積回数に関し、オンライン照会と指紋の一致の確認を行う条件を同じとしたが、これらを異なる条件としてもよい。また、この場合には、累積金額、累積回数は指紋の一致が確認できたときに初期化するようにしてもよい。

【0048】以上、本発明の第1、第2の実施形態によれば、不正による損害額が小さいと見積もられる場合には暗証番号のみの本人認証となるため、スーパーやコンビニエンスストアなどのお客さんの回転が早いお店でもスムーズに処理を行うことができる。一方、不正による損害額が大きくなる可能性があると思われる場合には指紋情報による本人認証も行うため、暗証番号が盗まれた場合でも不正使用を防ぐことが可能となり、高額な損害額の発生を防止することができる。また、指紋情報による本人認証と暗証番号による認証も行うため、生体情報による本人認証のみを行う場合に比べ生体情報による本人認証の精度が低くても、本人認証の信頼性はある程度確保できる。このため、生体情報による本人認証のためにICカードに記憶する生体情報の量や、生体情報の比較の処理のための負荷を低減することができる。

【0049】以下、本発明の第3の実施形態について説明する。

【0050】本第3実施形態は、前記第1実施形態における図3の処理を、図5に示すように、ステップ105で入力された暗証番号が間違っていた場合には、買い物金額が設定値を超えていない場合には（ステップ303）、指紋の比較（ステップ301、302）を行い、指紋が一致した場合には、暗証番号が間違っていたとしても本人認証が成立したものとし、買い物金額が設定値を超えている場合には（ステップ303）、指紋の比較（ステップ301、302）とオンライン照会（ステップ304）とを行い、その結果、指紋の一致と過去の不正無しとが確認できたならば暗証番号が間違っていたとしても本人認証が成立したものとする。ただし、暗証番号が間違っていた場合には、買い物金額が設定値を超えていない場合にもオンライン照会を行うようにしてもよい。また、図5の処理は、ユーザの選択に応じてステップ105の暗証番号の入力を省略し、常にステップ106で暗証番号が間違っていると判定させるようにすることにより、暗証番号の入力を省略したいユーザについては暗証番号の入力を求めないようにするようにしてもよい。

【0051】また、前記第2実施形態と同様に、累積金額や累積回数が設定値を超えている場合に、買い物金額が設定値を超えている場合と同様の処理を行うようにしてもよい。

【0052】以上、本第3実施形態によれば、前記第1、第2実施形態に対し、さらに、ユーザが暗証番号を忘れた場合にも、暗証番号を知らない、すなわち、疑義

あるユーザに対して本人認証を指紋を用いた本人認証により高い確度で行って、決済処理を行うことができるようになる。逆の見方をすれば、正当なユーザは暗証番号をもし忘れても、ICカードによる買い物をすることができるようになる。

【0053】以下、本発明の第4の実施形態について説明する。

【0054】本第4実施形態は、前記第3実施形態における図5の処理を、図6に示すように、ステップ105で入力された暗証番号が間違っていた場合に、指紋の比較（ステップ301、302）または指紋の比較（ステップ301、302）とオンライン照会（ステップ304）で本人認証が成立したならば、暗証番号の再登録を行うかを表示部3を介してユーザに問い合わせ（ステップ401）、暗証番号が入力部2により入力されたならば（ステップ402）、ICカード10の暗証番号記憶部15の暗証番号を入力された暗証番号に更新する（ステップ403）ようにしたものである。

【0055】なお、この場合は、買い物金額が設定値を超えていない場合にもオンライン照会を行うようにするのがよい。

【0056】また、前記第2実施形態と同様に、累積金額や累積回数が設定値を超えている場合に、買い物金額が設定値を超えている場合と同様の処理を行うようにしてもよい。

【0057】以上、本第4実施形態によれば、前記第3実施形態に対し、さらに、指紋を用いた本人認証によって高い確度でユーザを認証し、認証できたユーザに対しては、迅速、簡便な暗証番号の再登録サービスを提供することができるようになる。

【0058】以下、本発明の第5の実施形態について説明する。

【0059】図7に示すように、本第5実施形態は、前記第4実施形態における、図6の処理からステップ107～110、303、304を省略したものである。

【0060】すなわち、本第5実施形態では、買い物金額が設定値を超えているかどうかにかかわらず、入力された暗証番号が正しい場合には常に本人認証が成立したものとし、入力された暗証番号が間違っている場合にのみ指紋の比較（ステップ315、316）を行い、指紋が一致した場合には、暗証番号が間違っていたとしても本人認証が成立したものとする。なお、入力された暗証番号が間違っている場合には、オンライン照会を行うようにしてもよい。

【0061】これにより通常は暗証番号を用いた迅速な決済処理を行うことができる。また、ユーザが暗証番号を忘れた場合にも、暗証番号を知らない、すなわち、疑義あるユーザに対して本人認証を指紋を用いた本人認証により高い確度で行って、決済処理を行うことができる。逆の見方をすれば、正当なユーザは暗証番号をもし

忘れても、ICカードによる買い物をすることができるようになる。また、指紋を用いた本人認証によって高い確度でユーザを認証し、認証できたユーザに対しては、迅速な暗証番号の再登録サービスを提供することができる。

【0062】以上、本発明に係るICカード決済端末がクレジット端末である場合の実施形態を、第1～第5の実施形態として説明した。

【0063】以下、本発明に係るICカード決済端末が、電子マネーの決済を行うPOS端末である場合の実施形態を第6の実施形態として説明する。

【0064】図8に、本実施形態に係るPOS端末の構成について示す。

【0065】図中、17はPOS端末であり、26は購入者が使用するICカード、71は販売者が使用するICカードである。

【0066】また、POS端末中、18はキー入力部、19は表示部、20はレシートの印刷部、21は演算処理部、22はモデム部、23は取引履歴情報記憶部、24はICカード読み書き部、25は指紋読み取り部である。また、ICカード26中、27は接続部、28は演算処理部、29は金額情報記憶部、30はID情報記憶部、31は暗証番号記憶部、32は指紋情報記憶部である。ここで、金額情報記憶部29には、電子マネーとして使用可能な金額が記憶されている。なお、ICカード71の内部構成は、ICカード26と同様である。

【0067】このようなPOS端末17の動作について説明する。

【0068】図9に、POS端末17の演算処理部21が行う決済時の動作の手順を示す。

【0069】ただし、ここでは、既に販売者のICカード71がPOS端末17に装着され、既に販売者のICカード71についての本人認証は完了しているものとして説明する。

【0070】図示するように、POS端末17の演算処理部21は、購入者がICカード26をPOS端末17に挿入することにより装着すると（ステップ502）、販売者または購入者より、購入者のICカード26から販売者のICカード71に移動する電子マネーの金額である移動金額の入力を入力部18を介して受け付け（ステップ503）、その後、購入者より暗証番号の入力を入力部18を介して受け付ける（ステップ504）。

【0071】そして、暗証番号が入力されると、演算処理部21は、ICカード26の演算処理部28に暗証番号を渡し、入力された暗証番号と、ICカード26の暗証番号記憶部31に格納された番号とを比較させ、その結果より両者が一致したかを確認する（ステップ505）。そして、一致を確認できなかった場合には、ステップ507に進む。

【0072】一方、ステップ505で暗証番号の一致が

確認できた場合には、買い物金額があらかじめ設定した金額値を超えるかどうかの判定を行う（ステップ506）。そして、買い物金額があらかじめ設定した金額値を超えていない場合には、本人認証が成立したものととしてステップ509に進む。一方、買い物金額があらかじめ設定した金額値を超えている場合には、ステップ507に進む。

【0073】ステップ507では、指紋読み取り部25によりユーザーの指紋を読み取る。そして、演算処理部21は、ICカード26の演算処理部28に読み取った指紋の情報を渡し、これと、ICカード26の指紋情報記憶部32に格納された指紋情報とを比較させ、その結果より両者が一致したかを確認する（ステップ508）。そして、一致を確認できなかった場合には、ICカード読み書き部24にICカード26を排出させ（ステップ512）、処理を終了する（ステップ513）。

【0074】一方、ステップ508で指紋の一致を確認できた場合には、本人認証が成立したものととして、ステップ509に進む。

【0075】本人認証が成立した場合に行われるステップ509では、購入者用のICカード26の金額情報記憶部29に記憶されている電子マネーを、入力された移動金額分、販売者用のICカードの金額情報記憶部に移動することにより決済を行う。より具体的には、購入者用のICカード26の金額情報記憶部29に記憶されている電子マネーとして使用可能な金額を移動金額分減じ、販売者用のICカード71の金額情報記憶部に記憶されている電子マネーとして使用可能な金額を移動金額分増加させる。

【0076】次に、ステップ510では、POS端末17の取引履歴情報記憶部23に決済の内容を記憶する。たとえば、買い物の日付、買い物金額、買い物に使われたICカード26のID情報記憶部30に記憶されているIDなどを記憶する。そして、印刷部20によりレシートを発行する（ステップ511）と共に、ICカード26を排出して（ステップ512）、処理を終了する（ステップ513）。

【0077】以上、本発明の第6実施形態について説明した。

【0078】なお、以上では購入者用のICカード26から販売者用のICカード71に電子マネーを移動する場合について説明したが、本第6実施形態は、たとえば、電話回線を介して銀行からICカード26に電子マネーを移動する場合にも同様に適用することができる。この場合は、POS端末は、図8のステップ509において、モデム22を介して、銀行から移動金額分の電子マネーを受け取り、これをICカード26の金額情報記憶部29に記憶されている電子マネーに加える。

【0079】また、本第6実施形態は、前記第2実施形態と同様に、累積金額や累積回数を、ICカード26に記

憶し、これらが設定値を超えている場合に、移動金額が設定値を超えている場合と同様の処理を行うようにしてもよい。また、前記第1、第2実施形態のように、暗証番号が一致しなかった場合には、無条件に本人認証が成立しない者として、決済を行えないようにしてもよい。

【0080】また、暗証番号が一致しなかった場合にも指紋が一致した場合に本人認証が成立したとする場合には、前記第4実施形態と同様に、指紋の一致するICカードの所有者が、暗証番号の再登録をすることができるようにしたり、暗証番号の入力を省略したいユーザについては暗証番号の入力を求めないようにするようにしてもよい。

【0081】また、前記第5実施形態のように、買い物金額が設定値を超えているかどうかにかかわらず、入力された暗証番号が正しい場合には常に本人認証が成立したものとし、入力された暗証番号が間違っている場合にのみ指紋の比較を行い、指紋が一致した場合には、暗証番号が間違っているでも本人認証が成立したものとするようにしてもよい。

【0082】以上、本第6実施形態によれば、電子マネーの決済についても、前記クレジット端末に関する各実施形態と同様の効果を達成することができる。

【0083】さて、近年ではインターネットの普及により、パソコンを使ったインターネットショッピングが広まってきたが、この場合、電子マネーによる決済がセキュリティや手数料などの点でクレジット等と比べると優れている。

【0084】そこで、以下では、本発明に係るICカード決済端末が、電子マネーを用いたインターネットショッピングを行うパーソナルコンピュータである場合の実施形態を、第7の実施形態として説明する。

【0085】図10に、この場合のパーソナルコンピュータの構成を示す。

【0086】図中、33はパーソナルコンピュータ、42はICカードである。また、ICカード42中、43は接続部、44は演算処理部、45は金額情報記憶部、46はID情報記憶部、47は暗証番号記憶部、48は指紋情報記憶部、49は個人情報記憶部である。個人情報記憶部49にはICカード所有者の生年月日、年令、性別、国籍などの個人情報が記憶されている。また、パーソナルコンピュータ33中、34はキー入力部、35は表示部、36は印刷部、37は演算処理部、38はモデム部、39はカスタマイズ情報記憶部、40はICカード読み書き部である。カスタマイズ情報記憶部39には、個人情報に応じて、どのようにインターネットショッピングのユーザインタフェースをカスタマイズするかが記憶されている。ただし、パーソナルコンピュータ33中の各部は、パーソナルコンピュータ33が、所定のソフトウェアを実行することによりパーソナルコンピュータ33上に実現される機能部である。

【0087】さて、本実施形態では、インターネットショッピングの利便性を高めるために、ICカード42内の個人情報記憶部49にユーザーの個人情報を格納して、これらの情報によりインターネットショッピングに利用する画面の文字サイズ、言語、メニュー内容などを、ICカードの所有者に応じてカスタマイズする。

【0088】図11に、パーソナルコンピュータ33の演算処理部37が行う処理の手順を示す。

【0089】まず、ICカードを挿入されると（ステップ602）、ICカード42の個人情報記憶部49に格納された生年月日、年令、性別、国籍などの個人情報を読み取る（ステップ603）。

【0090】そして、センタと協調してモデム38を介してセンタからダウンロードされるデータを、読み取った個人情報に応じてカスタマイズし、表示部35より表示する（ステップ604）。カスタマイズする内容としては、ショッピングカタログの内容、文字サイズ、言語などがある。たとえば、若者と高齢者、女性と男性で、利用者に提供するショッピングカタログの内容を異なるものとする。

【0091】次に、利用者より購入する商品の番号と金額情報の入力を受け付けると（ステップ605）、次に利用者がICカード42の所有者本人であることを確認するために暗証番号の入力を受け付け（ステップ606）、暗証番号が一致した場合は、入力された金額分の電子マネーをセンタに移動する決済を行う（ステップ610）。また、間違った暗証番号が入力された場合には、指紋読み取り部41によりユーザーの指紋を読み取り（ステップ608）、ICカード42内の指紋情報記憶部48に格納された指紋情報と一致するかを確認し（ステップ609）、一致した場合は入力された金額分の電子マネーをセンタに移動する決済を行い（ステップ610）、取引履歴をパーソナルコンピュータに記憶する（ステップ611）。

【0092】そして、利用者より、買い物の終了が選択された場合（ステップ612）、及び、暗証番号も指紋も一致しなかった場合には、ICカード42を排出し（ステップ613）、処理を終了する（ステップ614）。買い物を続ける場合は、ステップ604よりの処理を行う。

【0093】以上、本発明の第7実施形態を説明したが、本第7実施形態において、前記第6実施形態と同様に、暗証番号が一致した場合にも、入力された金額が設置値より大きい場合には、さらに指紋の一致を確認し、一致した場合にのみ、ステップ608の決済を行うようにしてもよい。また、個人情報が示す年令が子供を示す場合には、アダルト情報にアクセスすることができないようにしてもよい。また、また、個人情報が示す年令が子供を示す場合には、低額の取り引きしか行えないように制限をかけるようにしてもよい。

【0094】なお、本第7実施形態における個人情報に
応じたユーザインタフェースのカスタマイズは、クレジ
ット端末、POS端末、電子マネーを取り扱う各種電子マ
ネー端末など、各種装置にも、同様に適用することがで
きる。

【0095】たとえば、図12に示すような、暗証番号
のみで本人認証を行う、オフラインで動作する電子財布
端末にも適用することができる。

【0096】図12において、50は電子財布端末であ
り、電子財布端末50中、51はキー入力部、52は表
示部、53は演算処理部、54はカスタマイズ情報記憶
部、55はICカード読み書き部である。また、56は
ICカードであり、ICカード56中、57は接続部、5
8は演算処理部、59は金額情報記憶部、60はID情
報記憶部、61は個人情報記憶部である。

【0097】電子財布端末50は、ICカードに格納さ
れた残高や取引履歴などの情報を表示するが、このと
き、ICカード56の個人情報記憶部61から読み出した
個人情報により文字サイズ、言語などをカスタマイズす
る。

【0098】なお、一般のパソコンのユーザインタフ
ェースのカスタマイズのみをICカードの個人情報により
行うようにすることも可能である。例えば、子供や高齢
者が操作する場合は、選択できる項目を減らしたり、高
機能なアプリケーションは選択できないようにすること
により、あまり迷わずに操作ができるようになる。

【0099】以下、本発明の第8の実施形態について説
明する。

【0100】本第8実施形態は、以上の各実施形態にお
ける指紋の読み取りに関するものである。

【0101】さて、指紋情報は警察での犯罪捜査に使わ
れていたことが多いため、ICカードの利用者の指紋情報
を読み取る際には生理的に不快感を伴うなどの問題が発
生しやすい。そこで、いかに利用者に不快感を与えない
ように読み取りを行うかが重要である。

【0102】そこで、本第8実施形態では、図13に示
すように、暗証番号を入力する数字キーに指紋読み取り
部を設けることにより、利用者にはあまり、指紋の読み
取りを意識をさせずに指紋を読み取ることができる。通
常、暗証番号は4桁以上であるため、数字キーに読み取
り部を設けた場合には、暗証番号の桁数と同一回数だけ
指紋を読み取ることができる。よって、複数の読み取り
データを用いて処理を行うことで精度を上げることも
可能となる。

【0103】一方、暗証番号の入力時には、数字キーに
よる入力後に必ず入力キー（エンターキー）を押すよう
にすることにより、図14に示すように、入力キーのみ
に指紋読み取り部も設けることも可能である。この場合
は、読み取り部は1個になるため、装置のコストを下げ
ることができる。

【0104】なお、ユーザーの指紋情報は、例えば右手
の人差し指から読み取るように統一させることも必要だ
が、例えば画面の右側にキーを配置して、さらにキーに
指の形状の窪みを設けることでユーザーに意識をさせな
くとも、ある程度は所望の指から指紋を取ることができ
るようになる。

【0105】いずれの場合も、指紋を読み取れなかった
場合には、画面にメッセージを出して利用者に説明を行
い、再度キーに指を載せて指紋を取得するようにしても
よい。

【0106】以上、本発明の実施形態について説明し
た。

【0107】なお、以上の第1実施形態から第7実施形
態では、本人認証に用いる生体情報として指紋を用いる
場合について説明したが、生体情報としては、掌紋、虹
彩、網膜など、その他の生体情報を用いるようにしても
よい。

【0108】また、以上の第1実施形態から第6実施形
態において、前記第7実施形態と同様にICカードにICカ
ードの所有者の個人情報を記憶し、ICカードに記憶した
個人情報を、生体情報の代わりに、もしくは、生体情報
と共に用いて本人認証を行うようにしてもよい。たとえ
ば、ICカード利用者から、誕生日や電話番号の入力を受
け付け、これと、ICカードに個人情報として記憶された
誕生日や電話番号とを比較し、両者が一致した場合に個
人情報による本人認証が成立したとするようにする。

【0109】

【発明の効果】以上のように、本発明によれば、本人認
証に要するコストと本人認証の確度との関係を本人認証
によって守るべき価値に応じて動的に最適化することが
できるICカード決済装置を提供することができる。

【0110】また、正当な所有者であれば、暗証番号を
忘れてしまった場合でも、ICカードを利用可能とするこ
とのできるICカード決済装置を提供することができる。

【0111】また、生体情報の取得に際して、ICカード
の所有者に与える不快感を軽減することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係るICカード決済端末
の構成を示すブロック図である。

【図2】本発明の第1実施形態に係るICカードに記録す
る取引履歴情報を示す図である。

【図3】本発明の第1実施形態に係るICカード決済端末
の動作を示すフローチャートである。

【図4】本発明の第2実施形態に係るICカード決済端末
の動作を示すフローチャートである。

【図5】本発明の第3実施形態に係るICカード決済端末
の動作を示すフローチャートである。

【図6】本発明の第4実施形態に係るICカード決済端末
の動作を示すフローチャートである。

【図7】本発明の第5実施形態に係るICカード決済端末

19

の動作を示すフローチャートである。

【図8】本発明の第6実施形態に係るICカード決済端末の構成を示すブロック図である。

【図9】本発明の第6実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図10】本発明の第7実施形態に係るICカード決済端末の構成を示すブロック図である。

【図11】本発明の第7実施形態に係るICカード決済端末の動作を示すフローチャートである。

【図12】本発明の第7実施形態に係るICカード決済端末の他の構成を示すブロック図である。

【図13】本発明の実施形態に係るICカード決済端末の指紋読み取り部を示す図である。

【図14】本発明の実施形態に係るICカード決済端末の指紋読み取り部を示す図である。

【符号の説明】

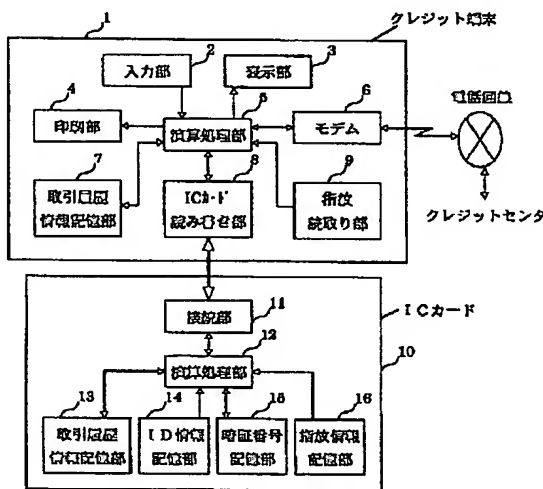
1…クレジット端末、2…入力部、3…表示部、4…印刷部、5…演算処理部、6…モデム部、7…取引履歴情報記憶部、8…ICカード読み書き部、9…指紋読み取り部、10…ICカード、11…接続部、12…演算処理部、13…取引履歴情報記憶部、14…ID情報記憶部、15…暗証番号記憶部、16…指紋情報記憶部、17…POS端末、18…入力部、19…表示部、20…印刷部、21…演算処理部、22…モデム部、23…取引履歴情報記憶部、24…ICカード読み書き部、25…指紋読み取り部、26…ICカード、27…接続部、28…演算処理部、29…金額情報記憶部、30…ID情報記憶部、31…暗証番号記憶部、32…指紋情報記憶部、33…パーソナルコンピュータ、34…入力部、35…表示部、36…印刷部、37…演算処理部、38…モデム部、39…カスタマイズ情報記憶部、40…ICカード読み書き部、41…指紋読み取り部、42…ICカード、43…接続部、44…演算処理部、45…金額情報記憶部、46…ID情報記憶部、47…暗証番号記憶部、48…指紋情報記憶部、49…個人情報記憶部、50…電子財布端末、51…入力部、52…表示部、53…演算処理部、54…カスタマイズ情報記憶部、55…ICカード読み書き部、56…ICカード、57…接続部、58…演算処理部、59…金額情報記憶部、60…ID情報記憶部、61…個人情報記憶部、7…ICカード

20

部、15…暗証番号記憶部、16…指紋情報記憶部、17…POS端末、18…入力部、19…表示部、20…印刷部、21…演算処理部、22…モデム部、23…取引履歴情報記憶部、24…ICカード読み書き部、25…指紋読み取り部、26…ICカード、27…接続部、28…演算処理部、29…金額情報記憶部、30…ID情報記憶部、31…暗証番号記憶部、32…指紋情報記憶部、33…パーソナルコンピュータ、34…入力部、35…表示部、36…印刷部、37…演算処理部、38…モデム部、39…カスタマイズ情報記憶部、40…ICカード読み書き部、41…指紋読み取り部、42…ICカード、43…接続部、44…演算処理部、45…金額情報記憶部、46…ID情報記憶部、47…暗証番号記憶部、48…指紋情報記憶部、49…個人情報記憶部、50…電子財布端末、51…入力部、52…表示部、53…演算処理部、54…カスタマイズ情報記憶部、55…ICカード読み書き部、56…ICカード、57…接続部、58…演算処理部、59…金額情報記憶部、60…ID情報記憶部、61…個人情報記憶部、7…ICカード

【図1】

図1



【図2】

図2

No.	取引日	引き当金	戻金	残高
1	98.9.15	8,000 円	19,800 円	3
2	98.9.18	4,000 円	11,800 円	2
3	98.9.12	7,800 円	7,800 円	1
4	98.9.10	22,000 円	51,900 円	3
5	98.9.5	14,800 円	29,800 円	2
6	98.9.4	15,800 円	15,300 円	1
7	98.9.2	7,500 円	22,000 円	6
8	98.8.20	2,000 円	14,500 円	4
.
.
.

【図13】

図13



図3

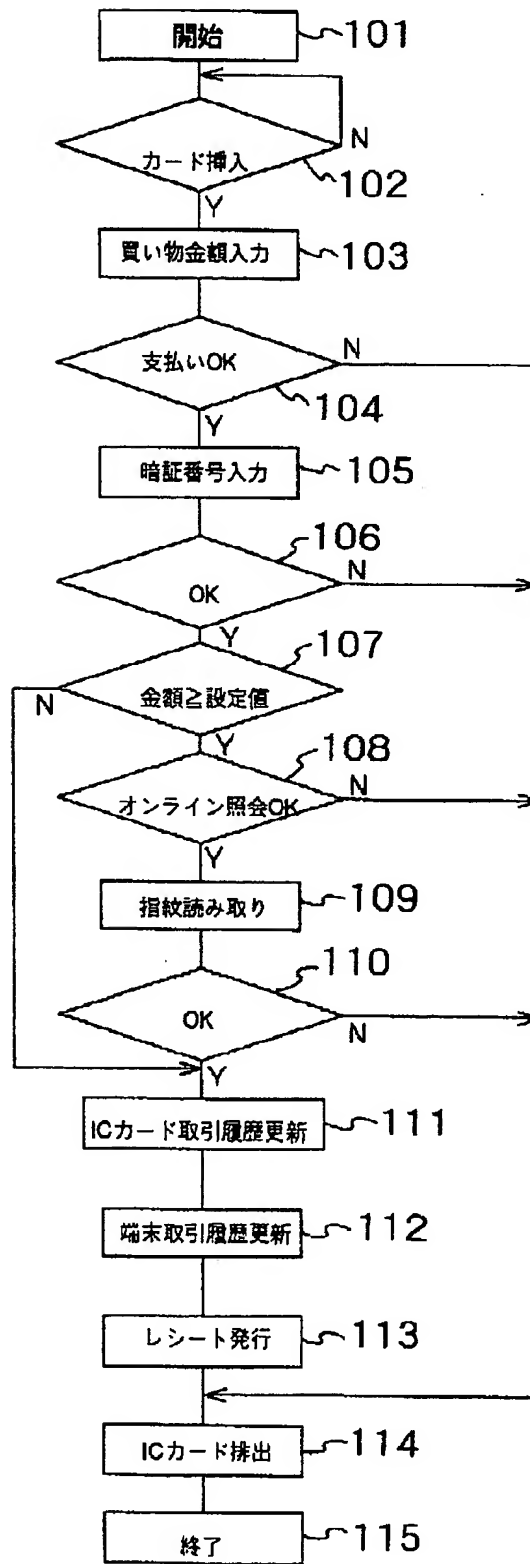
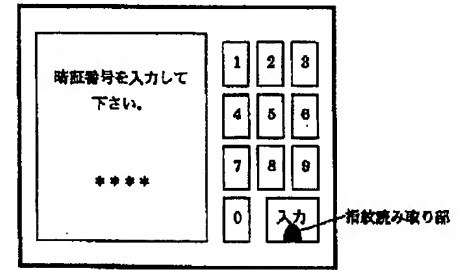
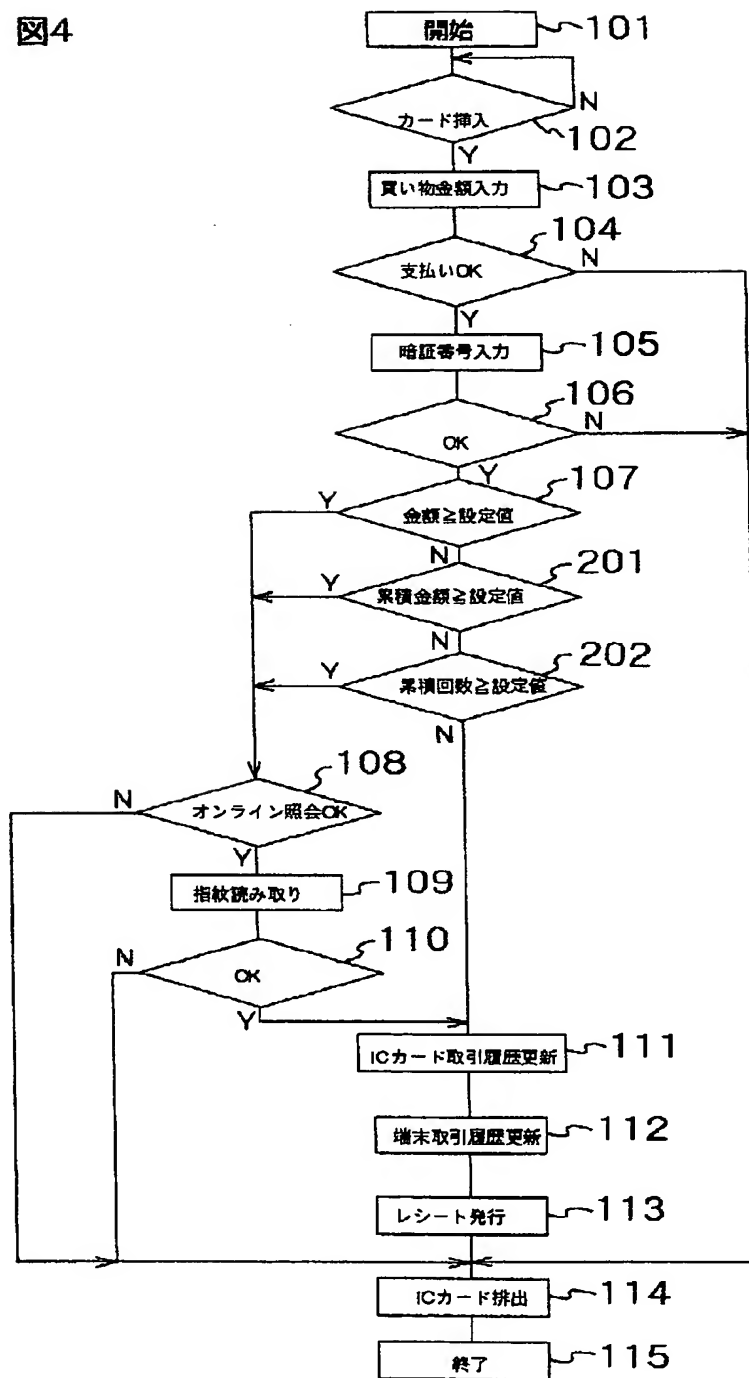


図14



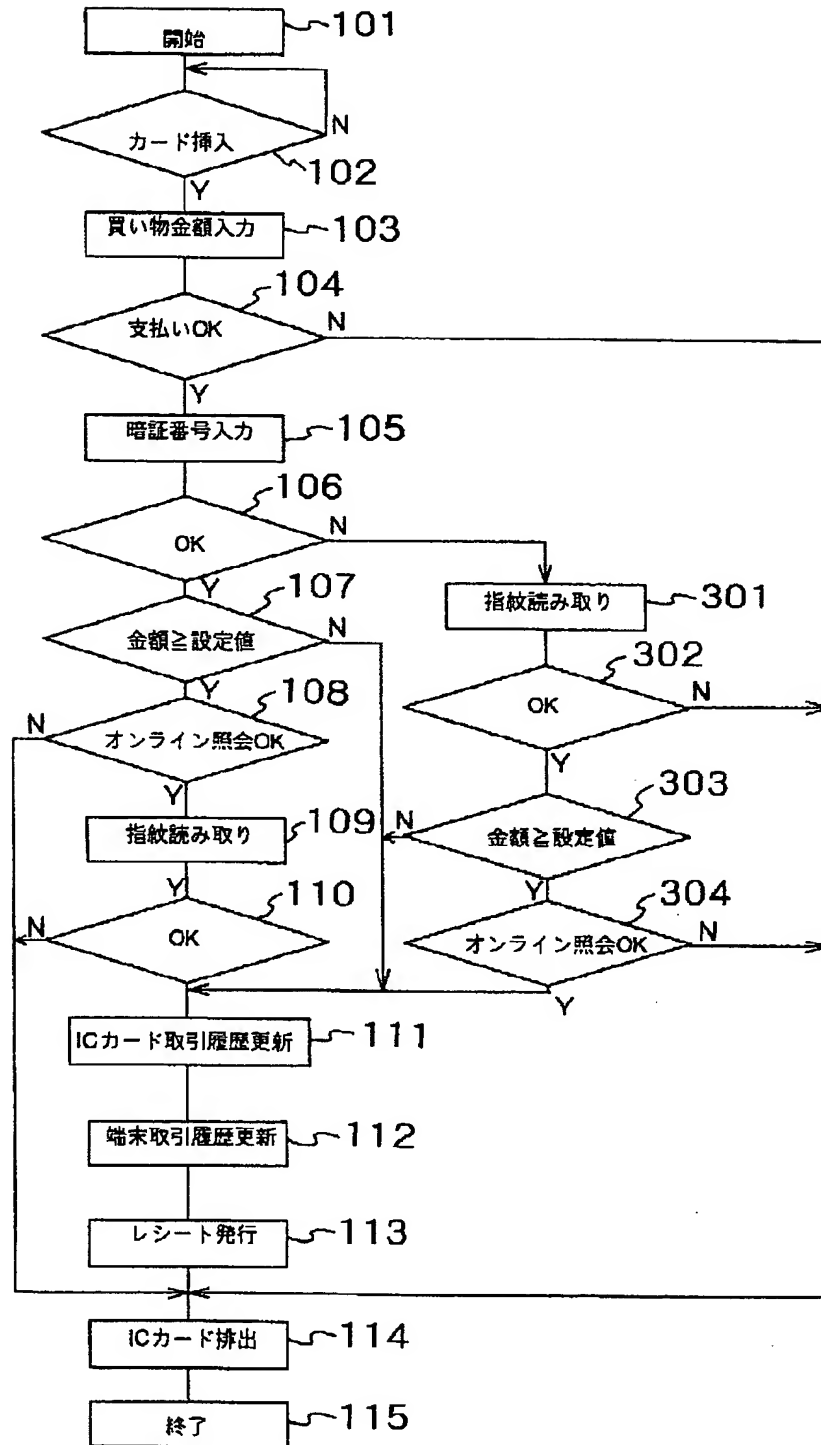
【図4】

図4



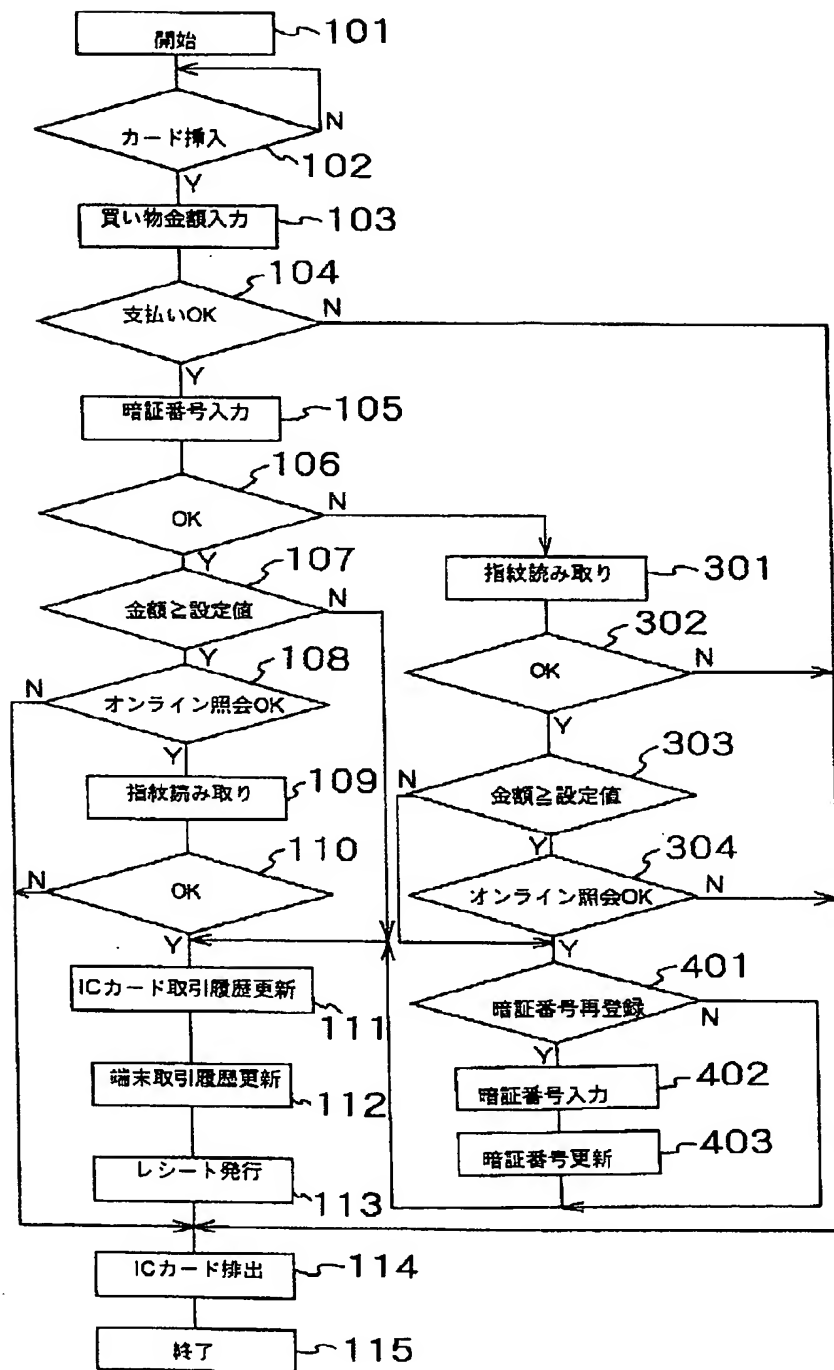
【図5】

図5

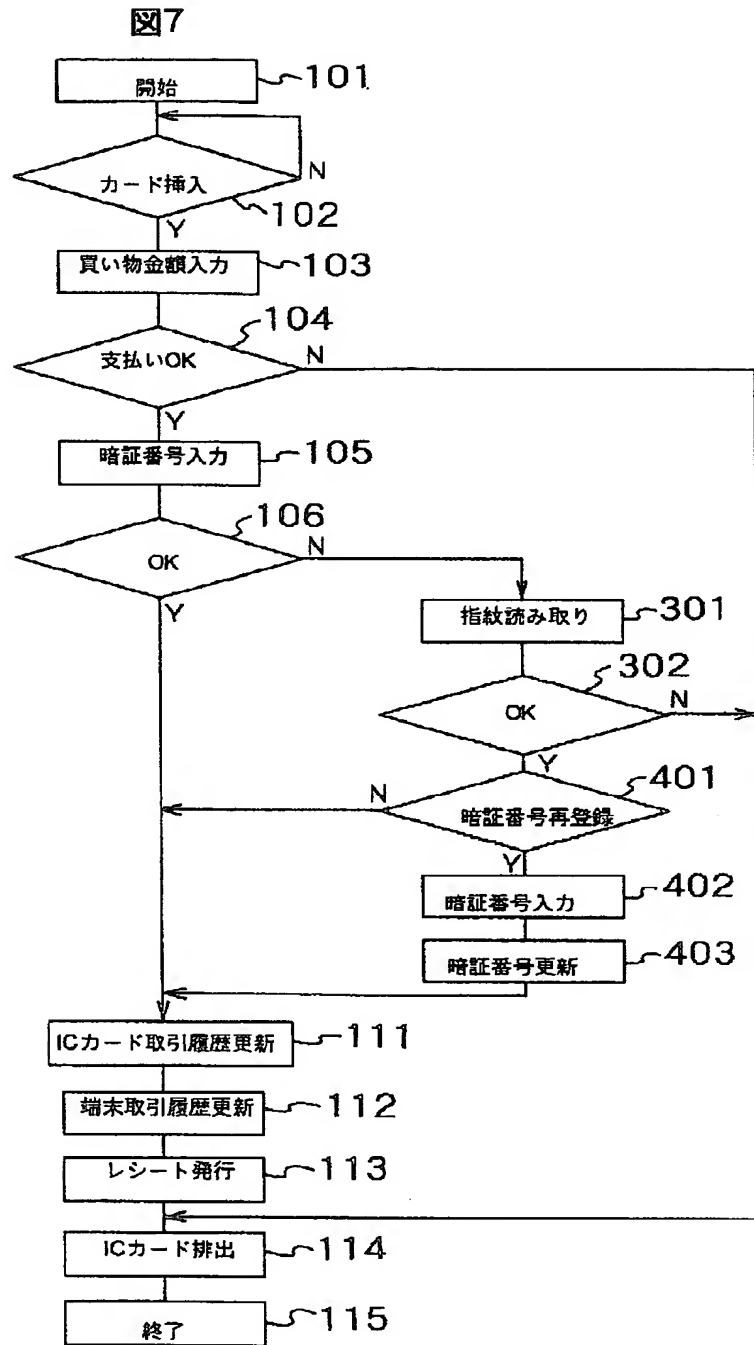


【図6】

図6

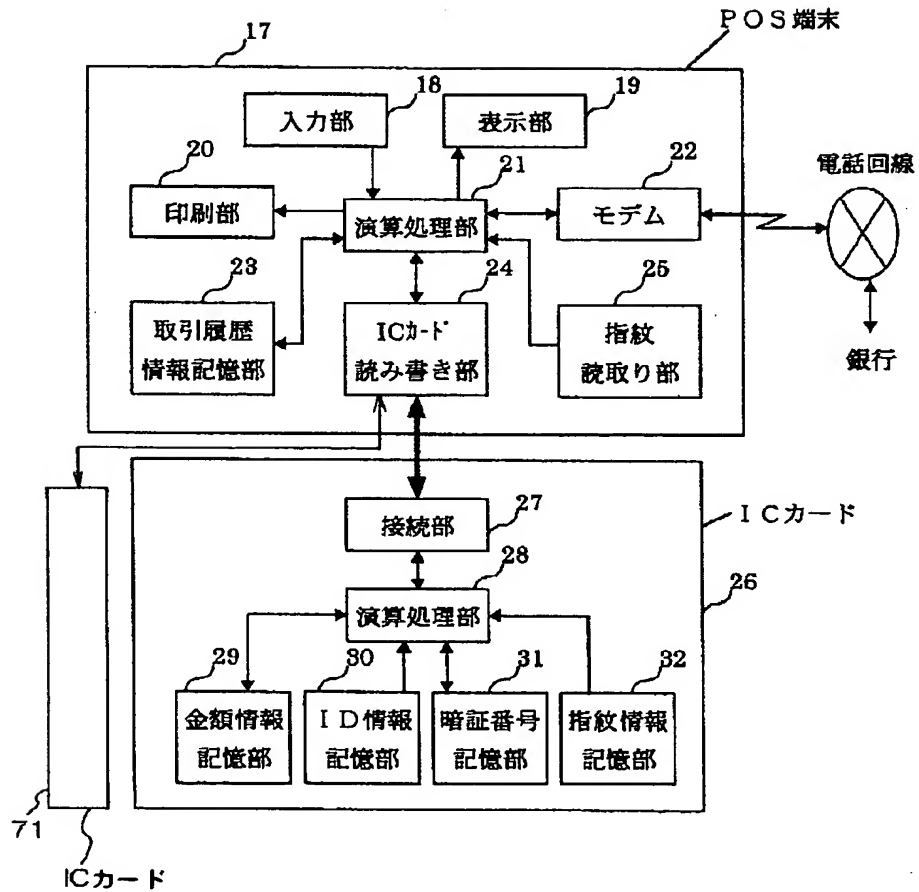


【図7】



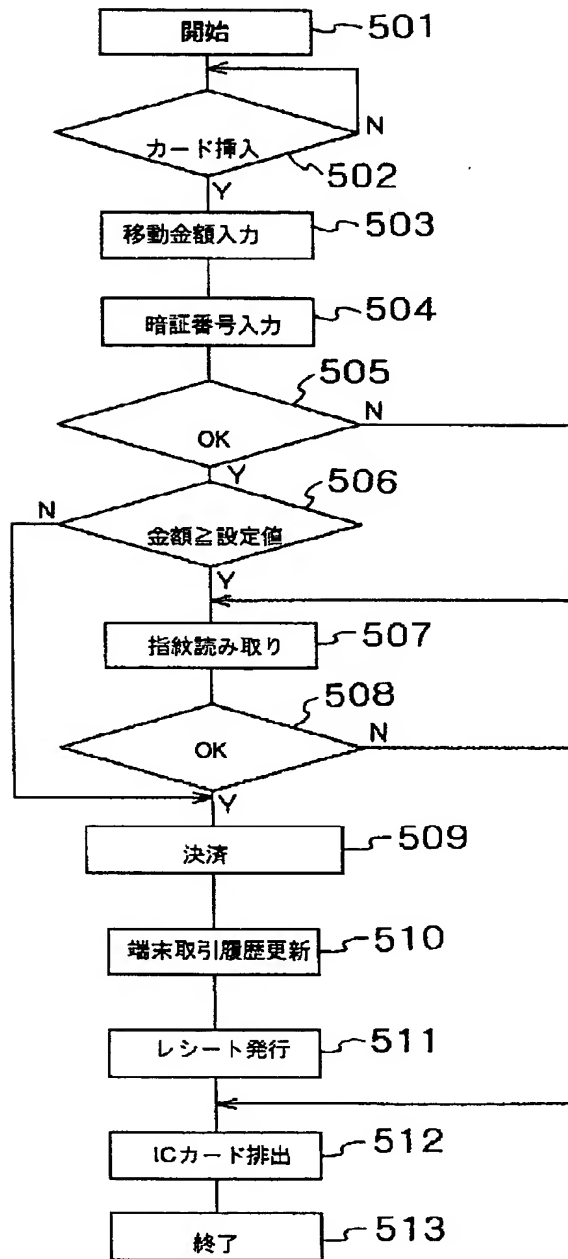
【図8】

図8



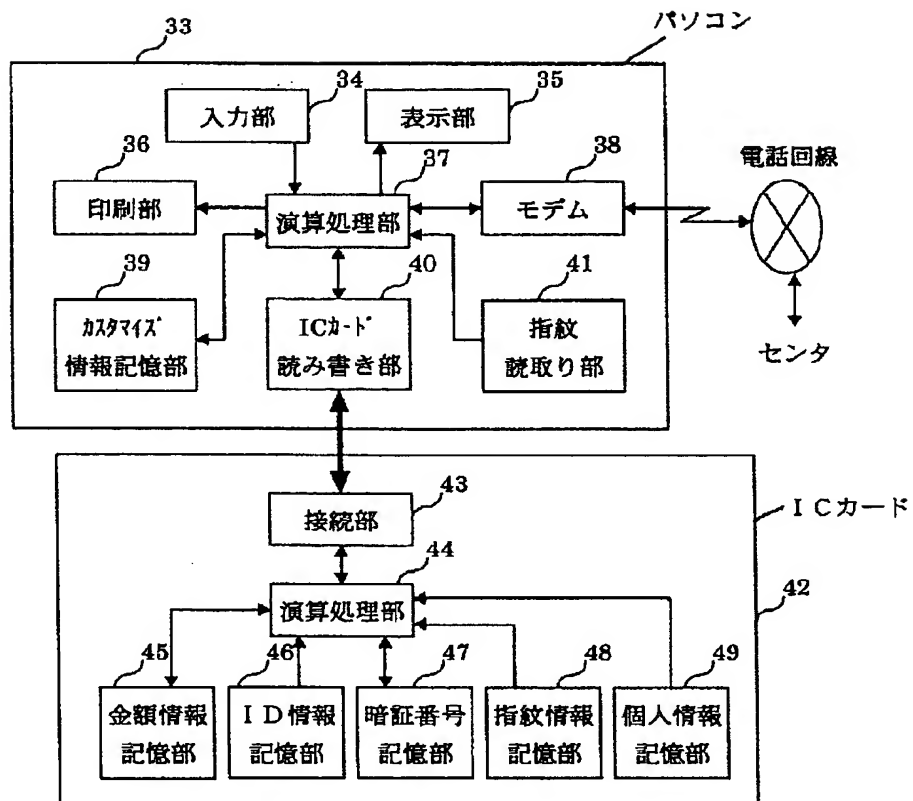
【図9】

図9



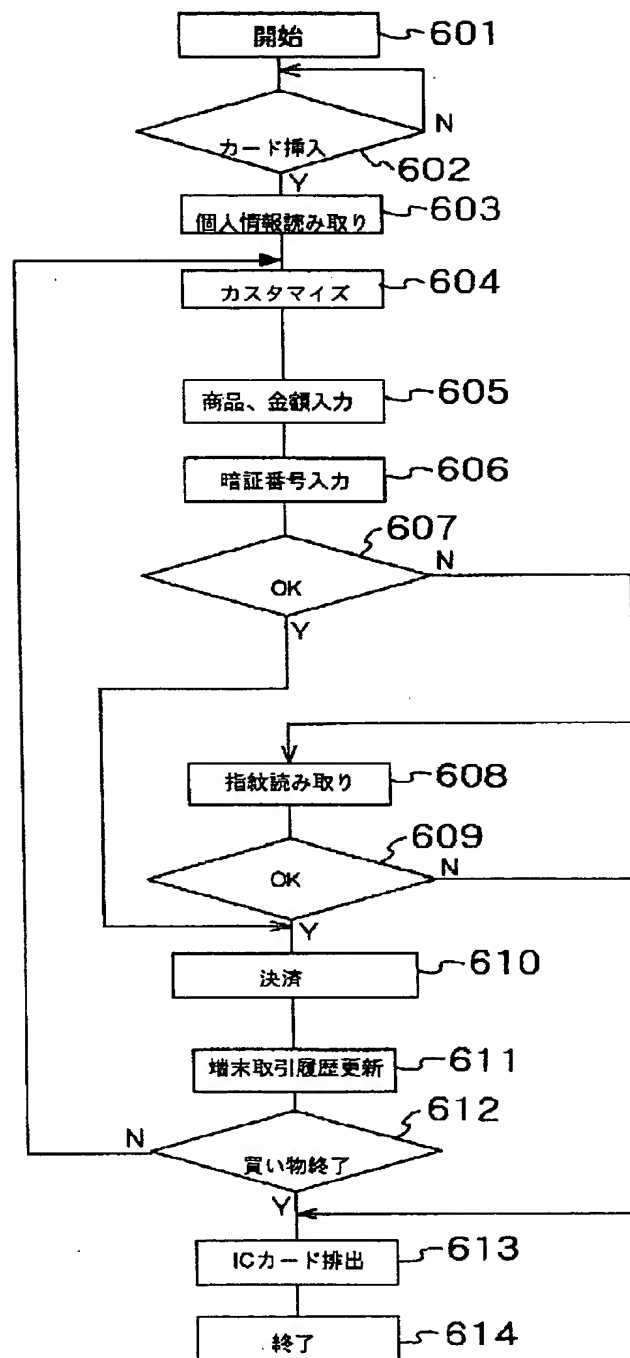
【図10】

図10



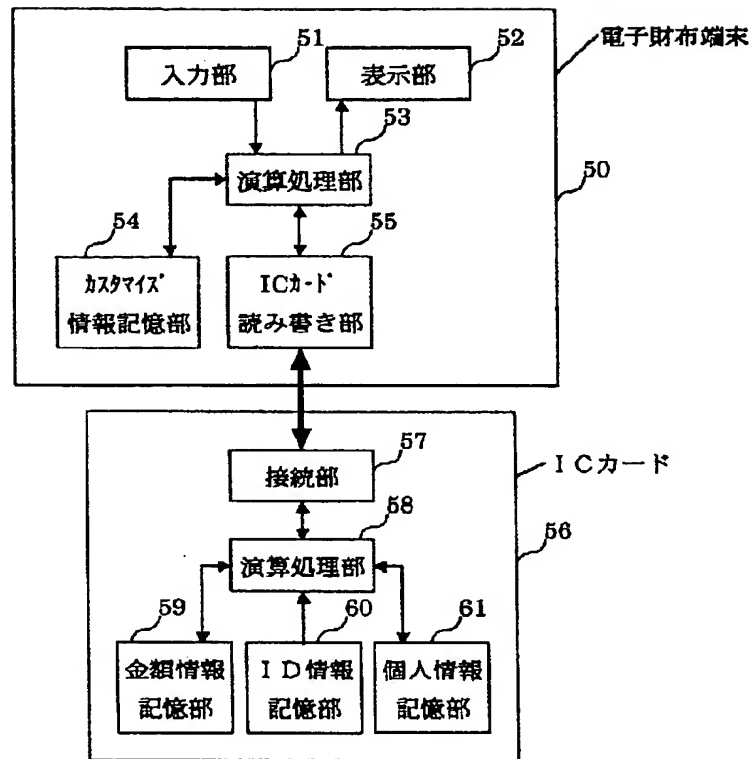
【図11】

図11



【図 12】

図12



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テ-マ-ド* (参考)
G 0 7 D 9/00	4 6 1	G 0 7 D 9/00	4 6 1 B
G 0 7 F 7/12		G 0 7 F 7/08	B
7/08			R
			Z

(72) 発明者 伊藤 滋行
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所マルチメディアシステム
開発本部内

(72) 発明者 高見 稔
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所マルチメディアシステム
開発本部内

(72) 発明者 井上 雅之
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立画像情報システム内

(72) 発明者 米田 幸一
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立画像情報システム内

(72) 発明者 稲光 哲治
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立画像情報システム内

(72) 発明者 山内 司
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所マルチメディアシステム
開発本部内

(72) 発明者 井上 喜男
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所マルチメディアシステム
開発本部内

F ターム (参考) 3E040 AA03 DA02 FK09
3E044 AA20 BA05 CA06 DA01 DA05
DA06 DB02 DB05 DC05 DC06
DD02 DE05
5B058 CA27 KA33 KA38 KA40 YA02